UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/480,231	01/10/2000	JORDAN YAAKOV LEVY	U 013180-1	4087

140 7590 03/26/2004

LADAS & PARRY
26 WEST 61ST STREET
NEW YORK, NY 10023

EXAMINER	
CHEN, SHIN HON	
ART UNIT	**PAPER NUMBER**
2131	13

DATE MAILED: 03/26/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/480,231	LEVY, JORDAN YAAKOV	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11,14 and 15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11,14 and 15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *January 10, 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☒ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6 and 11*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-11, 14, and 15 have been examined.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 4, 6, 8, 14, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant's Admitted Prior Art (hereinafter AAPA) in view of Kingdon U.S. Reissued Pat. No. RE37178 (hereinafter Kingdon) and further in view of Sakurai U.S. Pat. No. 5245657 (hereinafter Sakurai) and further in view of Swift et al. U.S. Pat. No. 6377691 (hereinafter Swift).

4. As per claim 1, 14, 15, AAPA discloses a method for verifying, by a verifier, that a prover has access to a private key associated with a public key Kp (AAPA: page 1 lines 30-32), the method comprising:

The prover sending an identification message to the verifier, the identification message comprising an indication of an identity of the prover, the indication of the identity including an indication of public key Kp (AAPA: page 2 lines 23-26);

Performing an identification round, the identification round comprising (AAPA: page 2 lines 23-27):

a. The verifier choosing a challenge Q (AAPA: page 3 line 1);

b. The prover selecting a random number R (AAPA: page 2 line 28), the random number is computed by applying a private disguising function Fv to Y, R being equal to Fv(Y) (AAPA: page 2 lines 9-13);

c. The prover sending a commit message to the verifier, the commit message comprising a disguised form of R produced by applying a function f to R, the disguised form of R being equal to f(R) (AAPA: page 2 lines 28-32);

d. The verifier sending a challenge message to the prover, the challenge message comprising the challenge Q (AAPA: page 3 line 1);

e. The prover sending a response message to the verifier, the response message comprising a response A, the response A satisfying a predicate relationship Pred(A,Q,f(R),Kp), wherein satisfying the predicate relationship provides an indication that the prover has access to the private key (AAPA: page 3 lines 1-4; page 1 lines 30-32); and

f. The verifier verifying that A satisfies the predicate relationship Pred(A,Q,f(R),Kp) (AAPA: page 3 lines 1-4); and

The verifier determining that the prover has access to the private key based on a result of the performing step ((AAPA: page 3 lines 1-4; page 1 lines 30-32).

AAPA does not explicitly disclose using padding string X. However, Kingdon discloses that limitation (Kingdon: column 5 lines 40-45: the remainder of the message is filled with zeroes). It would have been obvious to one having ordinary skill in the art to combine the teachings of Kingdon within the system of AAPA because the use of padding string enhances the security of a challenge by providing more bits to a message and makes it more difficult to decrypt.

The combination of AAPA-Kingdon does not explicitly disclose the verifier sending an initialization message to the prover, the initialization message comprising a disguised form Y produced by applying a public disguising function Fp to Q and X, Y being equal to Fp(Q,X); and the prover verifying that Y=Fp(Q,X). However, Sakurai discloses the verifier sending an enquiry formed by combining initial message with random message to the verifier and the verifier checks the enquiry has been correctly generated before generating a response (Sakurai: column 1 line 48 – column 2 line 5). It would have been obvious to one having ordinary skill in the art to combine the teachings of Sakurai within the combination of AAPA-Kingdon because it prevents the forging of verification transcript and it prevents verifier from impersonating the prover.

The combination of AAPA-Kingdon-Sakurai does not explicitly disclose the prover generating the random number based on input. However, Swift discloses that limitation (column 7 lines 39-62). It would have been obvious to one having ordinary skill in the art to combine the teachings of Swift within the combination of AAPA-Kingdon-Sakurai because the random number generated by the prover is more secure due to unpredictable and rapidly changing input.

5. As per claim 4 and 6, the combination of AAPA-Kingdon-Sakurai-Swift discloses the method according to claim 1. AAPA further discloses the use of one-way hash function as public or private disguising function (AAPA: page 2 lines 9-22).

6. As per claim 8, the combination of AAPA-Kingdon-Sakurai-Swift discloses the method according to claim 1. Sakurai further disclose the public disguising function Fp comprises a public key dependent disguising function Fpp dependent, in part, on the public key Kp, and Y is equal to Fpp(Q,X,Kp), and the prover verifying step comprises the prover verifying that Y=Fpp(Q,X,Kp) (Sakurai: column 1 lines 52-62). Same rationale applies here as above in rejecting claim 1.

7. Claims 2, 3, 5, 7, and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over AAPA in view of Kingdon and further in view of Sakurai and further in view of Swift and further in view of Shin et al. U.S. Pat. No. 5987134 (hereinafter Shin).

8. As per claim 2, the combination of AAPA-Kingdon-Sakurai-Swift discloses the method according to claim 1. AAPA-Kingdon-Sakurai-Swift does not explicitly disclose subsequent to the prover verifying that Y=Fp(Q,X), using the value Y of the verifier sending step in all subsequent operations using Y. However, Shin discloses that limitation (Shin: column 15 lines 26 and 33: F(n,e) is passed down to the next computation). It would have been obvious to one having ordinary skill in the art to combine the teachings of Shin within the combination of AAPA-Kingdon-Sakurai-Swift because it allows the result to be updated through out the process.

9. As per claim 3, the combination of AAPA-Kingdon-Sakurai-Swift discloses the method according to claim 1. AAPA-Kingdon-Sakurai-Swift does not explicitly disclose a method of performing the steps iteratively a plurality of times, and the verifier determining step includes determining based on a plurality of results each associated with one of the plurality of times that the performing step is performed. However, Shin discloses that limitation (Shin: column 3 lines 16-47: apply several calculations to generate response, each calculation is based on result of previous calculation). It would have been obvious to one having ordinary skill in the art to combine the teachings of Shin within the combination of AAPA-Kingdon-Sakurai-Swift because it increases the security by going through multiple rounds of computation.

10. As per claim 5 and 7, the combination of AAPA-Kingdon-Sakurai-Swift-Shin discloses the method according to claim 3. AAPA further discloses the use of one-way hash function as public or private disguising function (AAPA: page 2 lines 9-22).

11. As per claim 9, the combination of AAPA-Kingdon-Sakurai-Swift-Shin discloses the method according to claim 3. Sakurai further disclose the public disguising function Fp comprises a public key dependent disguising function Fpp dependent, in part, on the public key Kp, and Y is equal to Fpp(Q,X,Kp), and the prover verifying step comprises the prover verifying that Y=Fpp(Q,X,Kp) (Sakurai: column 1 lines 52-62). Same rationale applies here as above in rejecting claim 1.

12. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over AAPA in view of Kingdon and further in view of Sakurai and further in view of Swift and further in view of Hoffstein et al. U.S. Pat. No. 6076163 (hereinafter Hoffstein).

13. As per claim 10, the combination of AAPA-Kingdon-Sakurai-Swift discloses the method according to claim 1. AAPA-Kingdon-Sakurai-Swift does not explicitly disclose the function comprises R^2 modulo N. However, Hoffstein discloses that limitation (Hoffstein: column 2 lines 23-56). It is well known in the art to use modulo for computing commit message. Therefore, it would have been obvious to combine the teachings of Hoffstein within the combination of AAPA-Kingdon-Sakurai-Swift.

14. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over AAPA in view of Kingdon and further in view of Sakurai and further in view of Swift and further in view of Shin and further in view of Hoffstein.

15. As per claim 11, the combination of AAPA-Kingdon-Sakurai-Swift-Shin discloses the method according to claim 3. AAPA-Kingdon-Sakurai-Swift-Shin does not explicitly disclose the function comprises R^2 modulo N. However, Hoffstein discloses that limitation (Hoffstein: column 2 lines 23-56). It is well known in the art to use modulo for computing commit message. Therefore, it would have been obvious to combine the teachings of Hoffstein within the combination of AAPA-Kingdon-Sakurai-Swift-Shin.

Response to Arguments

16. Applicant's arguments with respect to claim 1-11, 14, and 15 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

17. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Kanda et al. U.S. Pat. No. 6044463 discloses method and system for message delivery utilizing zero knowledge interactive proof protocol.

Bush U.S. Pub. No. US2002/0002675 discloses secure encryption of data packets for transmission over unsecured networks and generation of pure random number embedded in one-time pad.

Goldwaser et al. U.S. Pat. No. 4926479 discloses multiprover interactive verification system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (703) 305-8654. The examiner can normally be reached on Monday through Friday 8:00am to 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon Chen
Examiner
Art Unit 2131

SC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100